

National Aeronautics and
Space Administration

John C. Stennis Space Center
Stennis Space Center, MS
39529-6000

SPD 2810.1 Rev. B
October 2010

COMPLIANCE IS MANDATORY

John C. Stennis Space Center Policy Directive Information Technology (IT) Network Security

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 15, 2010	
	Expiration Date: October 15, 2015	
Responsible Office: Center Operations Directorate		Page i of ii
SUBJECT: Information Technology (IT) Network Security		

Document History Log

[illegible]

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 15, 2010	
	Expiration Date: October 15, 2015	
Responsible Office: Center Operations Directorate		
SUBJECT: Information Technology (IT) Network Security		
Page ii of ii		

Table of Contents

1. POLICY	1
2. APPLICABILITY	2
3. AUTHORITY	2
4. APPLICABLE DOCUMENTS	3
5. RESPONSIBILITY	3
5.1 Center Director.....	3
5.2 Center Chief Information Officer	3
5.3 Directors, Program Managers, and Office Heads	4
5.4 IT Security Manager	5
5.5 Designated Approval Authority	6
5.6 Telecommunications Manager.....	6
5.7 Information System Owners	6
5.8 Center Chief of Security	7
5.9 Center Office of Human Capital Training Officer.....	7
5.10 Center Office of Procurement.....	7
5.11 Center IT Network Manager.....	8
5.12 SSCLAN Configuration Control Board.....	8
5.13 SSCLAN Firewall Configuration Control Board	8
5.14 NASA/SSC Contractors.....	8
5.15 SSC Employees and Visitors	9
6. CANCELLATION.....	9
APPENDIX A - ACRONYMS	10

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 15, 2010
	Expiration Date:	October 15, 2015
Page 1 of 10		
Responsible Office: Center Operations Directorate		
SUBJECT: Information Technology (IT) Network Security		

1. POLICY

- a. The John C. Stennis Space Center (SSC) shall develop and implement a comprehensive, but cost effective program for ensuring the security of Information Technology (IT) throughout its life cycle in accordance with federal, regulatory, and National Aeronautics and Space Administration (NASA) requirements.
- b. IT security encompasses the planning, acquiring, managing, controlling, and using SSC IT network resources to accomplish NASA and SSC's missions and programs efficiently, effectively, and securely.
- c. The policy shall supplement and enhance requirements for effective IT network security program management.
- d. IT network resources are defined as resources located at SSC and directly connected to a NASA managed network. The definition applies to all computers, wireless devices, Personal Digital Assistants (PDA's), routers, firewalls, switches, hubs, repeaters, gateways, and peripherals. Network resources encompass the data and information, computers, ancillary equipment, software, firmware and similar products; facilities that house such resources; operations, services; and related resources used for the acquisition, storage, manipulation, management, movement, control display, switching, interchange, transmission, or reception of data.
- e. SSC IT network resources shall be provided and managed consistent with acceptable risks, cost, and performance, as determined by SSC management to ensure that the resources are:
 - (1) Operated effectively and efficiently producing accurate data and information.
 - (2) Protected from unauthorized access, alteration, disclosure, destruction, loss, or misuse in operations and processing, storage and/or transmittal.
 - (3) Available to support critical SSC programs and functions.
 - (4) Incorporated with general management and hardware and software application controls sufficient to provide cost-effective acquisition, operation, and assurance of accuracy, integrity, and security.
 - (5) Provided with appropriate technical, personnel, administrative, environmental, and access safeguards before and after operational use.
 - (6) Operated in compliance with NASA and SSC policies and procedures.

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 15, 2010
	Expiration Date:	October 15, 2015
Page 2 of 10		
Responsible Office: Center Operations Directorate		
SUBJECT: Information Technology (IT) Network Security		

- (7) Operated in compliance with all software licensing conditions (as detailed by the registration/licensing agreements).
- (8) Provided with effective measures to ensure that software put to use is free of errors and viruses.

2. APPLICABILITY

- a. The policy defined herein applies to all NASA/SSC employees, NASA/SSC contractors, and to the extent appropriate Resident Agency organizations, in achieving NASA/SSC and Agency missions, programs, projects, and institutional requirements.
- b. Specifically, this document applies to all offices under the management of the SSC Center Director.
- c. Other co-located offices are encouraged to adopt this policy to ensure compatibility with systems and processes.

3. AUTHORITY

- a. 5 U.S.C. 552a, the Privacy Act of 1974, as amended.
- b. 18 U.S.C. 799, et. seq., Violation of Regulations of National Aeronautics and Space Administration.
- c. 18 U.S.C. 2510, et. seq., the Electronic Communications Privacy Act, as amended.
- d. 40 U.S.C. 759 note, the Computer Security Act of 1987, as amended.
- e. 42 U.S.C. 2451, et. seq., the National Aeronautics and Space Act of 1958, as amended.
- f. 44 U.S.C. 3541, et. seq., Federal Information Security Management Act of 2002
- g. Executive Order No. 12958, Classified National Security Information, as amended (March 2003).
- h. Executive Order No. 13011, Federal Information Technology of July 16, 1996.
- i. OMB Circular A-130, Management of Federal Information Resources, Appendix III.

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 15, 2010
	Expiration Date:	October 15, 2015
Responsible Office: Center Operations Directorate		
SUBJECT: Information Technology (IT) Network Security		

4. APPLICABLE DOCUMENTS

- a. NPD 1600.2, NASA Security Policy.
- b. NPD 2800.1, Managing Information Technology.
- c. NPR 2800.1, Managing Information Technology.
- d. NPD 2810.1, NASA Information Security.
- e. NPR 2810.1, Security of Information Technology.
- f. NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology.

5. RESPONSIBILITY

5.1 Center Director

The SSC Center Director shall have the oversight responsibilities for ensuring that an effective program for the management of IT is established and maintained for SSC. The Director ensures compliance with Government and NASA IT Directives and appoints:

- a. Center Chief Information Officer (CIO) to represent the Center on IT matters and coordinate with the NASA CIO to ensure the most effective and efficient oversight of implementation activities to support IT policies, architectures, standards, procedures, practices, initiatives, and services.
- b. Center IT Security Manager (ITSM) who provides organization and direction for implementing Center IT Security in coordination with the CIO.
- c. Designated Approval Authority (DAA) for accrediting information resources for processing national security information.

5.2 Center Chief Information Officer

The SSC CIO shall be responsible to establish an effective and economical IT Program at SSC as defined in NASA directives NPD 2800.1 and NPR 2800.1, Managing Information Technology and NPD 2810.1, NASA Information Security. The CIO responsibilities shall be to:

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 15, 2010
	Expiration Date:	October 15, 2015
Page 4 of 10		
Responsible Office: Center Operations Directorate		
SUBJECT: Information Technology (IT) Network Security		

- a. Establish, implement, and maintain computer architectures, standards, best practices, policies, and guidance to assure the secure operation of SSC Systems and the protection of SSC's data and information.
- b. Ensure the technical and security controls of SSC IT systems are appropriately implemented and maintained.
- c. Assure that the computer infrastructure has built-in recovery features (availability), provides adequate baseline protections (confidentiality), and protects data from modifications (integrity).
- d. Review the SSC IT network for alignment and compliance with Federal, NASA and SSC IT regulatory requirements, and directions.
- e. Coordinate and approve SSC's responses to required IT plans, budgets, reports, and audits.
- f. Participate in SSC's reengineering and continuous improvement processes by advocating the appropriate utilization of the IT network.
- g. Obtain and review metrics from SSC organizations relating to IT network planning, investment, returns, and appropriate utilization.
- h. Ensure the protection of all information (physical and electronic) and the SSC IT network resources and enforcing NASA information security policies and procedures and Federal information security policy.

5.3 Directors, Program Managers, and Office Heads

The Directors of SSC Directorates, Managers, and office heads shall:

- a. Plan, budget, and fund the acquisition, management, and use of IT resources under their direct management control and ensure the incorporation of IT security into the life cycle.
- b. Prepare data for integration into required SSC IT plans, reports, and audits.
- c. Assure compliance with Federal regulations, NASA directives, and SSC's IT network security program.
- d. Appropriate screening, approval, and training of personnel for the access and use of SSC IT resources.

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 15, 2010
	Expiration Date:	October 15, 2015
Page 5 of 10		
Responsible Office: Center Operations Directorate		
SUBJECT: Information Technology (IT) Network Security		

5.4 IT Security Manager

The ITSM shall be responsible for the overall management of the SSC IT Security Program and shall:

- a. Coordinate IT security activities with the CIO and developing and issuing directives necessary to implement the SSC IT Security Program.
- b. Support and coordinate with the Training Office to develop a SSC IT Security Awareness and Training Plan for implementing a training program that adheres to Agency initiatives and direction for IT security awareness and training.
- c. Establish a process to ensure that appropriate screening has been completed for individuals requesting system privileges.
- d. Conduct periodic reviews and compliance checks to ensure:
 - (1) SSC IT Security Plans are current or a plan for updating is in place.
 - (2) Significant changes to hardware, software, or operating environments are analyzed and documented for risk impact.
 - (3) SSC IT security policies and guidelines are current and comply with Federal and NASA regulations.
- e. Maintain documentation on SSC IT Security Plans, significant IT security incidents, audits, and evaluations; and establishing procedures for reporting metrics to management.
- f. Coordinate with the Center Chief of Security (CCS), Local Office of Inspector General (OIG), and the SSC IT Security Incident Response Team (IRT) to gather intelligence data regarding threats, concerns, and hacker techniques affecting the vulnerability of NASA information and systems.
- g. Respond appropriately to SSC IT security incidents by:
 - (1) Organizing and directing inquiries, examinations, and corrective actions.
 - (2) Maintaining a technically oriented IT IRT.
 - (3) Reporting incidents to SSC and Agency management and to the OIG, as necessary.
 - (4) Conducting penetration testing to ensure that controls are effective.

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 15, 2010
	Expiration Date:	October 15, 2015
Page 6 of 10		
Responsible Office: Center Operations Directorate		
SUBJECT: Information Technology (IT) Network Security		

5.5 Designated Approval Authority

The DAA shall be responsible for accrediting SSC information resources that process national security information (i.e., classified information). By accrediting a system, the DAA formally assumes responsibility for the operation of the system within a specified environment.

5.6 Telecommunications Manager

The SSC Telecommunications Manager shall be responsible for administering and managing SSC telecommunications functions encompassing infrastructure, voice and voice/data, facsimile, office automation desktop services, network connectivity, and radio and paging services. The Telecommunications Manager shall:

- a. Coordinate telecommunications activities with the CIO and develop/issue directives necessary to implement telecommunications requirements.
- b. Plan, budget, fund, and approve the acquisition, management, and use of telecommunications resources and services.
- c. Ensure telecommunications compliance with Federal regulations and NASA/SSC requirements and directions.

5.7 Information System Owners

Information System Owners (ISO's), designated by management, shall be responsible for the SSC IT Security Program for their systems. They serve as the critical communication link to and from their organizations for all IT security matters. The ISO's shall:

- a. Establish management controls and a communications process to ensure that SSC's implementation of the IT program and its security is consistent with mission needs and NASA policies and guidance.
- b. Serve SSC's representative to the ITSM and representing the SSC Line Managers (LM) on security matters.
- c. Report periodically to the ITSM and the organization's senior manager on the status of the IT security posture of systems under their purview.
- d. Ensure the preparation and annual review of SSC IT Security Plans for their Systems.
- e. Ensure that the security risks of SSC systems under their cognizance are identified and evaluated and that adequate safeguards are implemented.

Stennis Policy Directive	SPD 2810.1		B
	Number		Rev.
	Effective Date:	October 15, 2010	
	Expiration Date:	October 15, 2015	
	Page 7 of 10		
Responsible Office: Center Operations Directorate			
SUBJECT: Information Technology (IT) Network Security			

- f. Certify the adequacy and appropriateness of security controls before putting any new systems into operation. Periodically conduct the same certification throughout the life cycle of the system.
- g. Ensure that a properly trained System Administrator (SA) is assigned as the focal point for the security of each system or application.

5.8 Center Chief of Security

The SSC CCS shall be responsible for providing oversight, guidance, and approval authority for projects conducting classified activities. The CCS shall:

- a. Conduct appropriate personnel security screening for those working in sensitive positions and those who can bypass IT technical security controls and processes.
- b. Coordinate, investigate, and approve requests for foreign nationals who require access to systems, applications, and networks operated by or on behalf of NASA.
- c. Coordinate investigations of information security incidents and computer crimes, in conjunction with the CIO and/or ITSM.

5.9 Center Office of Human Capital Training Officer

The SSC Office of Human Capital Training Officer shall be responsible for coordinating with the ITSM to develop a SSC IT Security Awareness and Training Plan.

5.10 Center Office of Procurement

The SSC Office of Procurement shall be responsible for assuring that IT network acquisitions are approved and that appropriate security requirements are included in existing contracts, specifications and/or statements of work for IT security acquisitions or operations of IT installations, equipment, software, and related services. The Office of Procurement, working with the SSC CIO and the SSC ITSM, shall:

- a. Identify acquisitions for computer hardware, software, data management, and support services.
- b. Establish a joint process, with the SSC CIO and ITSM, to review acquisitions of SSC IT network resources.
- c. Ensure that all procurement actions, including solicitations and contracts, comply properly with IT network and IT security policies, procedures, and guidance.

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 15, 2010
	Expiration Date:	October 15, 2015
Page 8 of 10		
Responsible Office: Center Operations Directorate		
SUBJECT: Information Technology (IT) Network Security		

5.11 Center IT Network Manager

The SSC NASA IT Network Manager (ITNM) shall be responsible for the architectural, engineering, and security aspects of the SSC network. The ITNM shall:

- a. Enforce and monitor compliance with the network security policy.
- b. Provide direction to the NASA Network Control Contractor (NNCC) in the management of the SSC network.
- c. Monitor network traffic at SSC and investigating possible inappropriate traffic or connections.
- d. Serve as a member of the SSC Local Area Network (LAN) Configuration Control Board (CCB).
- e. Serve as a member of the SSC LAN Firewall CCB.

5.12 SSC LAN Configuration Control Board

The SSC LAN CCB shall provide overall policies for network design and architecture.

5.13 SSC LAN Firewall Configuration Control Board

The Firewall CCB shall be responsible for overseeing the firewall rules that define ports and services into SSC.

5.14 NASA/SSC Contractors

SSC Contractors shall be responsible for:

- a. Establishing the necessary management controls and a communications process to ensure that implementation and performance of the IT network activities is in accordance with requirements and all NASA/SSC policies and guidance.
- b. Performing appropriate screening, approval, and training of personnel for the access and use of SSC IT resources.
- c. Complying with SSC NASA IT security policies and procedures, and reporting IT security incidents or unauthorized access to the NASA IT Security Office.


Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date:	October 15, 2010
	Expiration Date:	October 15, 2015
Responsible Office: Center Operations Directorate		Page 9 of 10
SUBJECT: Information Technology (IT) Network Security		

5.15 SSC Employees and Visitors

All employees and visitors shall comply with SSC NASA IT security policies and procedures, and report IT security incidents or unauthorized access to the NASA IT Security Office.

6. CANCELLATION

None.



Patrick Scheurmann
Director

ATTACHMENTS

DISTRIBUTION

Approved for public release via NODIS and TechDoc; distribution is unlimited.

Stennis Policy Directive	SPD 2810.1	B
	<i>Number</i>	<i>Rev.</i>
	Effective Date: October 15, 2010	
	Expiration Date: October 15, 2015	
Responsible Office: Center Operations Directorate		
SUBJECT: Information Technology (IT) Network Security		

APPENDIX A - ACRONYMS

CCB	Configuration Control Board
CCS	Center Chief of Security
CFR	Code of Federal Regulations
CIO	Chief Information Officer
DAA	Designated Approval Authority
IRT	Incident Response Team
ISO	Information System Owner
IT	Information Technology
ITNM	Information Technology Network Manager
ITSM	Information Technology Security Manager
LM	Line Manager
NASA	National Aeronautics and Space Administration
NNCC	NASA Network Control Contractor
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements (formerly NPG, NASA Procedures and Guidelines)
OIG	Office of Inspector General
OMB	Office of Management and Budget
PDA	Personal Digital Assistant
SA	System Administrator
SPD	Stennis Policy Directive
SSC	Stennis Space Center
STD	Stennis Technical Standard
LAN	Local Area Network